SYSTEM AND METHOD FOR DETECTING BREACHED PASSWORDS WITHOUT DISCLOSING IDENTIFIABLE INFORMATION

BACKGROUND

The growth of the computing industry has been substantially driven by the continually expanding networking capabilities of computers and services offered by service providers over the Internet. Such growth and expansion of services has also created risks posed by hackers creating an increasing need for more comprehensive access security for given services and data. Service providers have established more rigorous password and authentication processes, which are designed to provide authorized use or access to sensitive data. These improved processes, however, also increase the complexity for entering and accessing the data. As a result of having more rigorous passwords and authentication processes, users can become frustrated when attempting to access services for which they use and/or pay.

One way in which hackers obtain access to users' sensitive data is by attempting to login to user accounts by trying different combinations of usernames and passwords. One way to limit the risk of intrusion is for a user to select a strong password. However, hackers have developed sophisticated tools for generating password and username combinations very quickly. Users have also become prone to using the same or similar passwords and usernames generally weakening otherwise strong passwords. Many of the passwords selected by users have been breached in attacks. Knowing whether a password, or a username, or a given username-password combination has been breached in an attack would help users select username and password combinations that have not already been breached and thus, lower the risk of getting hacked.

SUMMARY

In view of the above, systems and methods are provided to detect whether user login data is the subject of any breaches. In an example system, a network interface may be configured to communicate with a client device and a database of known web breach data. A hardware security module (HSM) includes a non-exportable key, and an HSM storage. The HSM performs a hashing function and a breach detection module. The breach detection module may be configured to receive breached web data elements from breached data providers. The breached web data elements may be hashed using a system key to generate breached web data hashes. The breached web data hashes are hashed in the HSM using the hashing method with the non-exportable key. Each hashed breached web data element may be stored in a hashed breached web database. The breach detection module receives at least one user login data hash. The at least one user login data hash may be received after being processed on the client device using the hashing method and an anonymous identifier from the client device. No information associated with a user of the client device is provided to the breach detection module.

The at least one user login data hash may be hashed in the HSM using the hashing method and the non-exportable key to generate at least one hashed user login data hash for each user login data hash. The breach detection module compares the at least one hashed user login data hash with each of the hashed breached web data elements. A breach notification may be sent to the client device for each hashed user login data hash that matches one of the hashed breached web data elements. The anonymous identifier and each hashed user login data hash that does not match any of the hashed breached web data elements may be stored for later status checks.

In an example computer-implemented method for detecting breached user login data in a zero-knowledge vault, breached web data elements are received from breached data providers. The breached web data elements are hashed using a hashing method with a non-exportable key. The hashed breached web data elements are stored in a hashed breached web database. At least one user login data hash and an anonymous identifier are received from a client device. The at least one user login data hash corresponds to user login data elements processed on the client device using the hashing method. No identifying information associated with a user of the client device is received by the breach detection module.

The at least one user login data hash may be hashed using the hashing method and the non-exportable key to generate at least one hashed user login data hash for each user login data hash. The at least one hashed user login data hash is compared with each of the hashed breached web data elements. A breach notification is sent to the client device for each hashed user login data hash that matches one of the plurality of hashed breached web data elements. The anonymous identifier and each hashed user login data hash that does not match any of the hashed breached web data elements are stored and sent to the client device. A random identifier may be generated and stored for each hashed user login data hash that does not match any of the hashed breached web data element. The random identifier may be sent to the client device.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. **1** is a block diagram of an example implementation of a system for detecting a breach of user login data, according to one embodiment.

FIG. **2** is a flow diagram illustrating operation of a method for detecting breached user login data, according to one embodiment.

FIG. **3** is a flow diagram illustrating operation of a method for detecting whether a user's login record is breached, according to one embodiment.

FIG. **4** is a flow diagram illustrating operation of a method for detecting whether a username and password combination has been breached after detecting a breach of the password, according to one embodiment.

FIG. **5** is a flow diagram illustrating the hash matching process performed by the hardware security module, according to one embodiment.

FIG. **6** is block diagram of another example implementation of a system for detecting a breach of user login data, according to one embodiment.

FIG. **7** is a block diagram of an example computer system that may be used in example implementations of a breach detection system.

DETAILED DESCRIPTION

Disclosed below are systems and methods for detecting whether a user's login data has been breached. The user login data that is of primary interest includes usernames, passwords, username-password combinations, and domains. The system can check whether a password and/or username has been breached by using a hash function to generate a first